# PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference PU030227	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/US2004/023940	International filing date *(day/month/year)* 27.07.2004	Priority date *(day/month/year)* 29.07.2003
International Patent Classification (IPC) or national classification and IPC H04L9/12		
Applicant THOMSON LICENSING S.A. et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *sent to the applicant and to the International Bureau)* a total of 3 sheets, as follows:

   ☒ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

   □ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. □ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☒	Box No. II	Priority
□	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
□	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
□	Box No. VI	Certain documents cited
□	Box No. VII	Certain defects in the international application
□	Box No. VIII	Certain observations on the international application

Date of submission of the demand 04.05.2005	Date of completion of this report 02.08.2005
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Cretaine, P Telephone No. +49 89 2399-8828

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US2004/023940

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   □ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   - □ international search (under Rules 12.3 and 23.1(b))
   - □ publication of the international application (under Rule 12.4)
   - □ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-7	as originally filed

Claims, Numbers

1, 3-14	received on 06.05.2005 with letter of 04.05.2005

Drawings, Sheets

1/2, 2/2	as originally filed

□ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☒ The amendments have resulted in the cancellation of:
   - □ the description, pages
   - ☒ the claims, Nos. 2
   - □ the drawings, sheets/figs
   - □ the sequence listing *(specify)*:
   - □ any table(s) related to sequence listing *(specify)*:

4. □ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - □ the description, pages
   - □ the claims, Nos.
   - □ the drawings, sheets/figs
   - □ the sequence listing *(specify)*:
   - □ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

Box No. II Priority

1. ☒ This report has been established as if no priority had been claimed due to the failure to furnish within the prescribed time limit the requested:
   - ☒ copy of the earlier application whose priority has been claimed (Rule 66.7(a)).
   - ☐ translation of the earlier application whose priority has been claimed (Rule 66.7(b)).

2. ☐ This report has been established as if no priority had been claimed due to the fact that the priority claim has been found invalid (Rule 64.1). Thus for the purposes of this report, the international filing date indicated above is considered to be the relevant date.

3. Additional observations, if necessary:

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1,3-14
	No:	Claims	
Inventive step (IS)	Yes:	Claims	1,3-14
	No:	Claims	
Industrial applicability (IA)	Yes:	Claims	1,3-14
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1: US-B1-6 526 506 (LEWIS DANIEL E) 25 February 2003 (2003-02-25)
D2:US 2002/164029 A1 (JIANG SAM SHIAW-SHIANG) 7 November 2002 (2002-11-07)

Closest prior art:

The document D1 is regarded as being the closest prior art to the subject-matter of claim 1, and shows (the references in parentheses applying to this document):

A key synchronisation method for a wireless network (see columns 12 and 13) comprising:

- setting a current encryption key ("ENCRYPT key") at an access point in the wireless network;

- generating a new encryption key ("new ENCRYPT key") at the access point;

- resetting the current encryption key to equal the newly generated encryption key;

- communicating the new encryption key to the station in an encrypted form using the previous encryption key (column 12, lines 45-47);

- the access point determining for each received data frame from the station if it is able to decrypt the data frame using the current encryption key.

Invention:

The subject-matter of claim 1 differs from this known method mainly in that a current encryption key and an old encryption key are maintained at the access point and that a data frame received from a station is either successfully decrypted with the current encryption key or a decryption failure is indicated and the frame is decrypted using the old encryption key.

The subject-matter of claim 1 is therefore new (Article 33(2) PCT).

The problem to be solved by the present invention may be regarded as how to enable the decryption of a received frame at the access point even if the key exchange with the station is not synchronized.

The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the reasons that none of the cited documents disclose or suggest to maintain the new and old encryption keys at the access station for the purpose of decryption.

Independent claim 8 relates to a system for performing the method of claim 1. Claim 8 therefore also meets the requirements of Article 33 PCT.

Claims 3-7 and 9- 14 are dependent on claims 1 or 8 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Remarks:

Claim 8 lacks clarity, due to the use of the wordings "mechanism" and "using" in that claim.

The claims are not numbered consecutively, contrary to Rule 6.1(b) PCT.

CLAIMS

1. A key synchronization method for a wireless network comprising:

setting a current encryption key and an old encryption key at an access point in the wireless network;

generating a new encryption key at the access point;

resetting the current encryption key to equal the newly generated encryption key;

resetting the old encryption key to equal an encryption key being used by a station in communication with the access point;

communicating the new encryption key to the station in an encrypted form using the old encryption key; and

indicating a decryption failure for a data frame received from the station when the encryption key used by the station does not match the current encryption key, wherein a data frame that failed to decrypt using the current encryption key is decrypted using the old encryption key.

2. Cancelled

3. The method according to claim 1, further comprising:

incrementing an out-of-sync counter in the access point when said decrypting fails due to the station encryption key not matching the current key; and

decrypting received data frames associated with said out-of-sync counter at the access point using the old encryption key.

4. The method according to claim 1 , further comprising:

decrypting, using the new key, the received data frame from the station when the access point determines the station sending the received packet is using the new key, said access point starting to use the new key when a first data frame correctly encrypted with the new key is received from the station;

re-setting the old key to equal the current key when decryption is successful; and

re-setting an out-of-sync counter to zero upon successful decryption.

5. The method according to claim 1, further comprising setting the old key equal to a null value, said null value representing a no encryption mode.

6. The method according to claim 1, further comprising setting the current key and the first key to a null value, said null value representing a no encryption mode.

7. The method according to claim 1, wherein said step of setting is performed by the access point for each station in the wireless network.

8. A key synchronization mechanism for a wireless network comprising:

at least one station in the wireless network; and

at least one access point in the wireless network maintaining an old encryption key and a new encryption key through a key rotation interval for each of said at least one station, said access point using said new encryption key when a first data frame correctly encrypted with said new key is received from said at least one station and using said old encryption key when decryption of a data frame received from said at least one station fails due to mismatched keys.

9. The key synchronization mechanism according to claim 8, wherein said at least one access point further maintains an out-of-sync counter to track the number of packets where decryption fails due to mismatched keys.

10. The key synchronization mechanism according to claim 8, wherein said at least one access point is capable of setting the old encryption key to a null value, said null value representing a no encryption mode.

11. The key synchronization mechanism according to claim 8, wherein said at least one access point is capable of setting the new encryption key to a null value, said null value representing a no encryption mode.

12. The key synchronization mechanism according to claim 8, wherein said at least one access point initially sets the old encryption key to a null value.

13. The method according to claim 1, wherein the new encryption key is generated at the access point upon expiration of a key refresh interval.

14. The method according to claim 3, wherein said out-of-sync counter comprises a predetermined threshold that if exceeded causes the termination of communication between the access point and a source of the data frames causing the threshold of said out-of-sync counter to be exceeded.